Optimised Rabbit Code

Erik Zenner

Technical University Denmark (DTU)
Institute for Mathematics
e.zenner@mat.dtu.dk

FSE 2008, Feb. 12, 2008

About Rabbit

The Rabbit stream cipher:

- Presented at FSE 2003
- Commercial design (IPR held by Cryptico)
- Free for non-commercial purposes
- No known attacks (128-bit security)
- High software performance claimed
- *eStream* finalist in the software category

Code Availability

Until 2005:

- Only reference code publicly available.

Since 2005:

- Partially optimised code publicly available (eStream web page).

Since February 2008:

- Fully optimised (commercial) code publicly available (eStream web page).

First Observations

Cryptico's observations:

- Keystream generation performance improved by factor 2.5 to 3.5.
- Key/IV setup performance improved by factor 1.5 to 3.0.

Dan Bernstein's first measurements:

- Pentium Core 2 Duo: 2.34 cycles/byte
- Pentium M: 3.94 cycles/byte
- Athlon 64 X2: 2.86 cycles/byte

First Observations

Cryptico's observations:

- Keystream generation performance improved by factor 2.5 to 3.5.
- Key/IV setup performance improved by factor 1.5 to 3.0.

Dan Bernstein's first measurements:

- Pentium Core 2 Duo: 2.34 cycles/byte
- Pentium M: 3.94 cycles/byte
- Athlon 64 X2: 2.86 cycles/byte

Feel free to do your own testing!